攻防博弈驱动下的无线传感器网络病毒传播模型 *

周海平 [1]，沈士根 [1]，黄龙军 [1]，刘 妮 [2]

(1. 绍兴文理学院 计算机科学与工程系，浙江 绍兴 312000; 2. 贵阳学院 数学与信息科学学院，贵阳 550005)

摘 要：传统的无线传感器网络（wireless sensor networks，WSN）病毒传播模型直接给定感染概率和恢复概率，没有对其取值的原因进行分析。从博弈论的角度对 WSN 中病毒传播的微观机理进行分析，建立了 WSN 的攻防博弈模型，求出了博弈模型的混合纳什均衡解，并根据博弈双方的混合纳什均衡策略确定节点的感染概率和治愈概率，从而建立了 WSN 的病毒传播模型。此外，还进一步使用元胞自动机的方法对 WSN 的病毒传播过程进行模拟，理论分析及计算机模拟揭示了病毒传播结果与博弈参数之间的关系，研究结果对制定抑制病毒传播的措施具有一定的指导意义。

关键词：无线传感器网络；病毒传播；攻防博弈；元胞自动机模拟

中图分类号：TP393 doi: 10.19734/j.issn.1001-3695.2018.08.0650

Virus propagation model for wireless sensor networks driven by attack-defense game

Zhou Haiping[1], Shen Shigen[1], Huang Longjun[1], Liu Ni[2]

(1. *Dept. of Computer Science & Engineering, Shaoxing University, Shaoxing* Zhejiang 312000, *China*; 2. *Dept. of Mathematic & Information Science, Guiyang College, Guiyang* 550005, *China*)

Abstract: In traditional virus propagation models on Wireless Sensor Networks (WSN), the infection probability and recovery probability are given directly, and are lack of analysis of the reasons for its value. From the perspective of the game theory, this paper analyzed the microscopic mechanism of virus propagation in WSN. By building and analyzing the attack-defense game model, it obtained the mixed Nash equilibrium solution of the model. With the solution, it deduced the infection probability and cure probability and then established the theoretical model for virus propagation in WSN. Meanwhile, this paper simulated viruses' propagation process with cellular automata method. The theoretical analysis and simulation results revealed the relationship between the propagation speed and the game parameters. The results of this study are of significance for people to formulate measures to suppress the propagation of viruses.

Key words: wireless sensor networks; propagation of virus; attack-defense game; cellular automaton

0 引言

随着物联网技术的技术的发展，WSN 已经成功地应用于交通运输、环境监测、军事侦查等多个领域[1,2]。然而，由于无线传感器节点的存储和计算能力十分有限，很容易受到恶意程序的攻击[3,4]。常见的攻击方式有信道干扰、身份欺骗、病毒传播等多种形式[5,6]。其中恶意病毒传播是一种更为严重的攻击方式，因为一旦某个节点被病毒感染，该节点又会进一步向其他节点传播，导致网络迅速崩溃[7,8]。

至今为止，人们已经分别对 WSN 的攻防检测及恶意程序传播问题进行了大量研究。WSN 的攻防研究方面，张可径等人从博弈论的角度分析了恶意节点与防御系统之间的攻防策略，然后利用演化动力学方法得到了攻防双方的博弈均衡解，对 WSN 的防御过程有一定的指导价值[9]。刘怡等人针对工业 WSN 的能耗攻击问题提出了基于演化博弈的攻防模型，得到了博弈双方的进化稳定策略，为能耗攻击的防御策略提供了可行策略[10]。文献[11]使用数据挖掘技术对 DoS 攻击进行特征识别，并采用特征选择算法进一步提炼关键特征，该方法在降低时间复杂度的同时提高了 DoS 攻击的识别率。在病毒传播研究方面，郑榕俊等人利用传染病动力学理论对 WSN 中多种蠕虫病毒传播的行为进行了研究[12]，得到了多种病毒交互作用时的网络传播特性。文献[13]将传统的传染病传播理论应用于 WSN 中的恶意程序传播过程，作者将恶意程序和入侵检测系统（intrusion detection system, IDS）当作两种相互对抗的智能体，建立了二者之间的微分博弈模型，通过对博弈模型的分析和求解，得到了二者之间的均衡策略，该策略可以在抑制恶意程序的传播的同时降低检测代价。文献[14]提出了一个含个体差异的病毒传播模型，该模型中不同的节点具有不同的抗攻击能力，研究结果显示节点抵抗能力的异质性对病毒传播效果有显著影响。文献[15]对 WSN 中的移动代理被攻击时病毒的传播过程进行了研究，发现在移动代理被攻击的情况下病毒更容易扩散。

在已有的针对 WSN 恶意程序传播的研究中，人们在建立传播模型时通常直接给定节点的感染概率和治愈概率，而没有考虑其背后的微观机理。而对于一个真实的 WSN 网络来说，感染概率和治愈概率与攻击方和防御方所采取的策略有关，基于这个原因，本文从博弈论的角度分析攻防双方的策略，并基于该策略来确定感染概率和治愈概率，从而揭示博弈参数对传播效率的影响。论文结构安排如下：a）建立 WSN 中攻防双方的博弈模型，并求取模型的纳什均衡策

收稿日期：2018-08-14；**修回日期：**2018-10-22 **基金项目：**国家自然科学基金资助项目（61772018）

作者简介：周海平（1978-），男，江西宜春人，教授，博士，主要研究方向为复杂网络、无线传感器网络(hpzhou2885@163.com)；沈士根（1974-），男，浙江桐乡人，教授，博士，主要研究方向为博弈论、网络安全；黄龙军（1976-），男，福建连城人，讲师，博士，主要研究方向为无线传感器网络，刘妮（1983-），女，贵州开阳人，副教授，硕士，主要研究方向为网络安全.

略;b）基于攻防双方的博弈策略建立 WSN 的 SIS 病毒传播模型，通过求解传播模型得到病毒传播速度与博弈参数之间的关系;c）对理论模型进行数值模拟及仿真，并将仿真结果与理论模型的解析结果进行比较与分析。

1 WSN 的攻防博弈模型

WSN 中含有恶意节点与合法节点，其中恶意节点是指感染了病毒的节点，会向合法节点传播病毒，合法节点会利用 IDS 对接收的信息进行检测。合法节点利用 IDS 对信息进行检测需要消耗一定的能量，由于节点能量有限，合法节点若对接收的所有信息都进行检测则很快会因能量耗尽而无法工作，为了延长其使用寿命，合法节点会以一定的概率对接收的信息进行检测。对于恶意节点来说，如果其频繁地发起攻击，则很快会暴露自己的身份，因此恶意节点也会以一定的概率发起攻击，由此可见，合法节点与恶意节点之间的攻防过程其实是一种博弈，因此本文利用博弈理论分析它们之间的攻防策略。

定义 1 WSN 中攻防双方的博弈模型可以表示为一个三元组 $\Xi=[N,\{S_i\},\{u_i\}]$，其中：

a)N 为博弈的参与者集合，对于 WSN 来说，$N=\{$合法节点，恶意节点$\}$。

b)S_i 为参与者的策略集合，当 i 为合法节点时，$S_{合法节点}$={检测，不检测}，当 i 为恶意节点时，$S_{恶意节点}$={攻击，不攻击}，需要特别指出的是，此处的不攻击策略不是指恶意节点不发送任何信息，而是指其发送正常信息。

c)u_i 为参与者 i 在博弈过程中获得的收益，u_i 的值由博弈双方所采取的策略决定。表 1 给出了本文用到的一些符号的定义，表 2 给出了博弈双方的收益矩阵。

表 1 符号定义

Table 1 Symbolic definition

符号	含义
a	合法节点检测到病毒获得的收益，恶意节点被识别造成的损失。
b	恶意节点攻击成功带来的收益，合法节点感染病毒造成的损失。
e_S	合法节点对收到的信息进行检测所需的能量代价。
e_I	恶意节点发送病毒或正常信息所消耗的能量代价。
x	恶意节点发起攻击的概率。
y	合法节点进行检测的概率。
Eu_S	合法节点在攻防博弈中的期望收益。
Eu_I	恶意节点在攻防博弈中的期望收益。

表 2 合法节点与恶意节点的博弈收益表

Table 2 Game payoff for legitimate node and malicious node

合法节点	恶意节点	
	攻击	不攻击
检测	$a-e_S$，$-a-e_I$	$-e_S$，$-e_I$
不检测	$-b$，$b-e_I$	0，$-e_I$

为了使博弈有意义，模型须满足 $a\ge e_S$ 及 $b\ge e_I$ 这两个条件，因此，当恶意节点发起攻击时合法节点的最佳策略就是进行检测，反之就不进行检测；对于恶意节点来说，当合法节点进行检测时，其最佳策略就是不进行攻击，反之就进行攻击。由于攻防双方互不知道对方会采取何种行动，上述博弈模型不存在纯策略纳什均衡解，下面从混合均衡策略的角度分析博弈双方的攻防行为。

定理 1 WSN 中的攻防博弈模型存在混合纳什均衡策略。

证明 假设恶意节点以概率 x 进行攻击（传播病毒），以概率 $1-x$ 不进行攻击（传播正常信息），合法节点以概率 y 进行检测，以概率 $1-y$ 不进行检测，则根据收益矩阵，合法节点的期望收益 Eu_s 为

$$Eu_s=xy(a-e_S)+(1-x)y(-e_S)+x(1-y)(-b) \tag{1}$$

恶意节点的期望收益 Eu_I 为

$$\begin{aligned}Eu_I&=xy(-a-e_I)+(1-x)y(-e_I)\\&+x(1-y)(b-e_I)+(1-x)(1-y)(-e_I)\end{aligned} \tag{2}$$

令 $\frac{\partial Eu_S}{\partial y}=0$，得

$$x(a-e_S)+(1-x)(-e_S)-x(-b)=0 \tag{3}$$

整理上式得
$$x=\frac{e_S}{a+b} \tag{4}$$

当 $x=\frac{e_S}{a+b}$ 时，$\frac{\partial Eu_S}{\partial y}=0$，合法节点进行检测的期望收益等于不进行检测的期望收益；

当 $x>\frac{e_S}{a+b}$ 时，$\frac{\partial Eu_S}{\partial y}>0$，合法节点进行检测的期望收益大于不进行检测的期望收益；

当 $x<\frac{e_S}{a+b}$ 时，$\frac{\partial Eu_S}{\partial y}<0$，合法进行检测的期望收益低于不进行检测的期望收益。

同理，令 $\frac{\partial Eu_I}{\partial x}=0$，得

$$\begin{aligned}&y(-a-e_I)-y(-e_I)+\\&(1-y)(b-e_I)-(1-y)(-e_I)=0\end{aligned} \tag{5}$$

整理上式得
$$y=\frac{b}{a+b} \tag{6}$$

当 $y=\frac{b}{a+b}$ 时，$\frac{\partial Eu_I}{\partial x}=0$，恶意节点发起攻击的期望收益等于不攻击的期望收益；

当 $y>\frac{b}{a+b}$ 时，$\frac{\partial Eu_I}{\partial x}<0$，恶意节点发起攻击的期望收益低于不攻击的期望收益；

当 $y<\frac{b}{a+b}$ 时，$\frac{\partial Eu_I}{\partial x}>0$，恶意节点发起攻击的期望收益高于不攻击的期望收益。

由以上分析可知，合法节点会根据恶意节点的攻击概率决定是否进行检测，而恶意节点也应该根据合法节点进行检测的概率决定是否发起攻击，$\left(x^*=\frac{e_S}{a+b},y^*=\frac{b}{a+b}\right)$ 便是恶意节点与合法节点进行攻防博弈的混合纳什均衡策略。证毕。

2 博弈驱动下的 WSN 病毒传播模型

由博弈模型可知，恶意节点和合法节点作为理性个体分别会以概率 x^* 和概率 y^* 进行攻击和检测，当恶意节点发起攻击而合法节点又没有进行检测时，合法节点就会被感染，而当恶意节点攻击时合法节点开启了检测，则恶意节点会被清除病毒并恢复为合法节点。因此，合法节点被感染的概率为 $x^*(1-y^*)$，而恶意节点被治愈的概率为 x^*y^*。假设恶意节点占网络中总节点的比例为 i，合法节点占网络中总节点的比例为 s，则 WSN 中的病毒传播演化模型可以用方程组(7)描述。

$$\begin{cases}\frac{di}{dt}=x^*(1-y^*)si\text{-}x^*y^*si\\ \frac{ds}{dt}=-x^*(1-y^*)si+x^*y^*si\\ i+s=1\end{cases} \tag{7}$$

于是有
$$\frac{di}{dt}=x^*(1-2y^*)i(1-i) \quad (8)$$

即
$$\frac{di}{i(1-i)}=x^*(1-2y^*)dt \quad (9)$$

令 $t_0=0$，并假设初始时刻的感染比例为 i_0，对方程(9)从 t_0 到 t 进行积分得

$$\ln\frac{i_t}{1-i_t}-\ln\frac{i_0}{1-i_0}=x^*(1-2y^*)t \quad (10)$$

对方程(10)进一步求解可得

$$i_t=\frac{i_0}{i_0+(1-i_0)e^{-x^*(1-2y^*)t}} \quad (11)$$

将 $x^*=\frac{e_S}{a+b}$，$y^*=\frac{b}{a+b}$ 代入上式得

$$i_t=\frac{i_0}{i_0+(1-i_0)e^{-\frac{(a-b)e_S}{(a+b)^2}t}} \quad (12)$$

由式(12)可知，病毒的传播过程最终由博弈模型的收益参数决定。通过对式(12)进行数值模拟，得到博弈参数与网络节点感染比例之间的关系如图 1~3 所示。当 $a>b$ 时（图 1），网络节点的感染比例会随时间的推移达到 1，意味着网络中所有节点最终都会被病毒感染，并且此时病毒传播的速度随检测能耗 e_S 的增大而变快；当 $a=b$ 时（图 2），感染比例维持初始值不变，并且不受检测能耗 e_S 的变化所影响；当 $a<b$ 时（图 3），网络节点的感染比例会随时间的推移达到 0，意味着病毒将会在网络中彻底消失，并且此时病毒传播的速度随检测能耗 e_S 的增大而变慢。

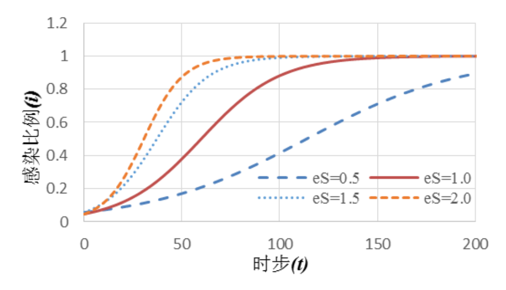


图 1 $a>b$ 时感染节点比例随时间的变化趋势（a=3.0,b=2.0）

Fig. 1 Trend of infection node ratio over time for a>b（a=3.0,b=2.0）.

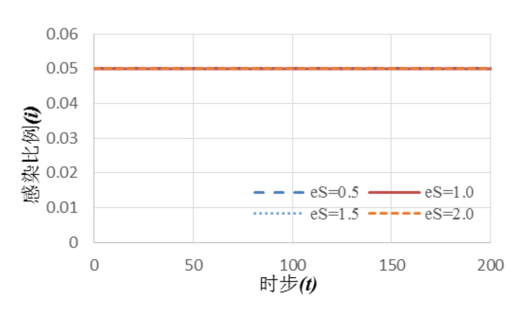


图 2 $a=b$ 时感染节点比例随时间的变化趋势（a=2.0,b=2.0）

Fig. 2 Trend of infection node ratio over time for a=b（a=2.0,b=2.0）.

3 元胞自动机模拟

前面的理论模型虽然可以较好地描述 WSN 中恶意程序传播的过程，但仍然存在一些局限，例如，真实的传感器节点的通信半径是有限的，节点只能与其附近的节点通信，而理论模型没有考虑这个问题，另外对于有些传感器网络来说，节点可以移动，因此网络是动态变化的，现有的理论模型也无法处理这个问题。为了使研究结果与真实场景更接近，本节使用元胞自动机方法对 WSN 的病毒传播过程进行模拟。

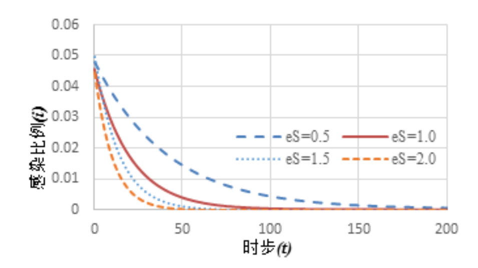


图 3 $a<b$ 时感染节点比例随时间的变化趋势（a=2.0,b=3.0）

Fig. 3 Trend of infection node ratio over time for a<b（a=2.0,b=3.0）.

3.1 模拟步骤

a)生成一个如图 4 所示的 100×100 的网格，随机选择比例为 p_w 的格子布设传感器节点.

b)任意两个传感器节点之间的距离如果不超过 r 则产生连接关系，由此确定传感器网络的结构。

c)在初始时刻，随机设置比例为 i0 的节点为恶意节点。

d)每个恶意节点随机选择一个与其直接相连的节点发送信息，其中发送恶意信息的概率为 x^*，发送正常信息的概率为 $1-x^*$。

e)当恶意节点向恶意节点发送信息时，信息会被丢弃，而当恶意节点向合法节点发送信息时，合法节点会以概率 y^* 进行检测。当合法节点接收到的是病毒且正好没有进行检测时就会被感染，当合法节点对收到的病毒进行检测时，恶意节点会被识别，被识别的恶意节点会被修复，从而又转换为合法节点。

f)若 t 小于预设的模拟步数，则 t 的值增加 1，并转入步骤 d)继续执行，否则，结束运行。

3.2 模拟结果

设定参数 p_w=0.1，i_0=0.05，执行上述模拟步骤，考查博弈参数对病毒传播结果的影响。模拟结果如图 5~7 所示。从图中可以看出，当 $a>b$ 时，随着时间的推移，网络中恶意节点的比例不断增加，最终所有节点都被病毒感染，并且病毒的传播速度随检测能耗 E_S 的增大而加快；当 $a=b$ 时，随时间的推移，网络中恶意节点的比例始终在初始感染比例附近上下波动；当 $a<b$ 时，随着时间的推移，网络中恶意节点的比例不断减少，最终所有节点都变为合法节点。该结论与上一节的理论研究结果一致。

另外，由于 WSN 中病毒的传播过程与通信半径有关，本文进一步研究了传感器节点的通信半径对病毒传播速度的影响，通过改变通信半径的值，得到了不同通信半径下病毒的传播曲线，从图 8 可以看出，在其他参数固定的情况下，病毒的传播速度随着通信半径的增加而增大。

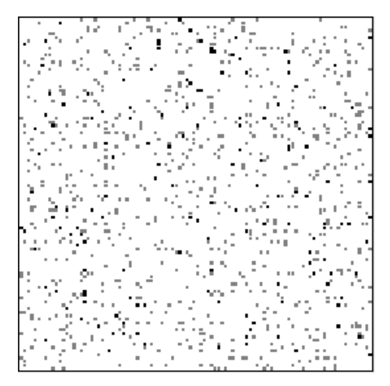


图 4 无线传感器节点分布图（灰色为正常节点，黑色为恶意节点）

Fig. 4 Distribution of wireless sensor nodes (gray presents normal node, blackpresents malicious node)

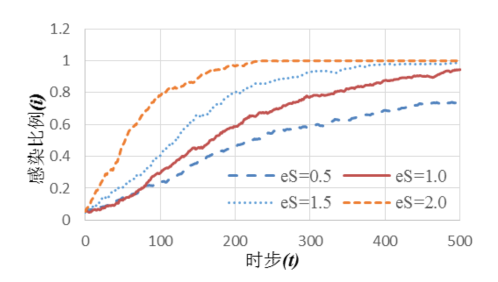


图 5　*a*>*b* 时感染节点比例随时间的变化趋势（*a*=3.0,*b*=2.0,*r*=5）

Fig. 5　Trend of infection node ratio over time for *a*>b

（*a*=3.0,*b*=2.0,*r*=5）

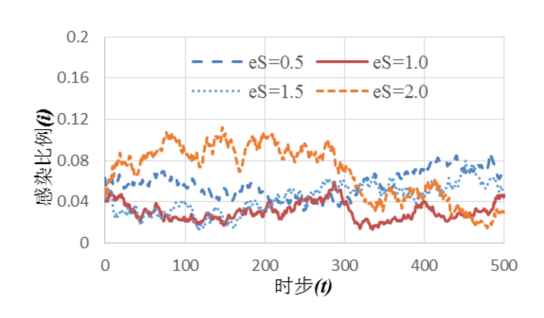


图 6　*a*=*b* 时感染节点比例随时间的变化趋势（*a*=2.0,*b*=2.0,*r*=5）

Fig. 6　Trend of infection node ratio over time for *a*=b

（*a*=2.0,*b*=2.0,*r*=5）

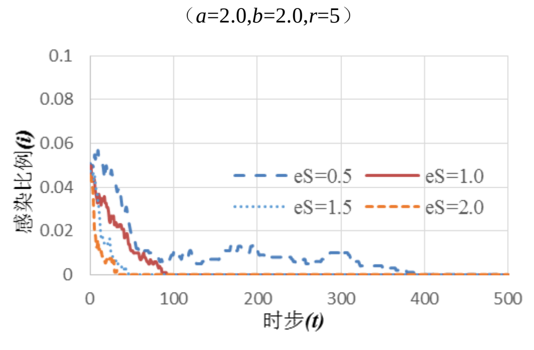


图 7　*a*<*b* 时感染节点比例随时间的变化趋势（*a*=2.0,*b*=3.0,*r*=5）

Fig. 7　The trend of infection node ratio over time for *a*<b

（*a*=2.0,*b*=3.0,*r*=5）

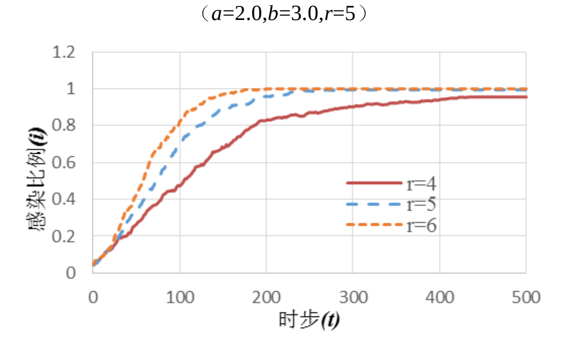


图 8　通信半径对病毒传播速度的影响（e_S=2.0,*a*=3.0,*b*=2.0）

Fig. 8　Influence of communication radius on virus propagation speed.

（e_s=2.0,*a*=3.0,*b*=2.0）

4　讨论

4.1　理论结果与模拟结果的比较

从整体规律上看，前面的理论研究结果和元胞自动机模拟的结论是一致的，但是在细节上还是会有一些差异，例如：在 a>b 时，理论模型中病毒的传播速度要大于元胞自动机模拟的传播速度，其原因如下：a）理论模型中任意两节点之间是直接相连的，节点之间可以充分混合，而元胞自动机模型中只有距离相近的节点才能直接通信，当某个节点附近的节点都已经被感染时，就不能进一步传播病毒;b）在元胞自动机模型中，随着传播的进行，恶意节点之间会聚集成簇，这种聚集效应也会阻碍病毒迅速传播。

4.2　博弈参数对病毒传播过程的影响

本文的研究揭示了博弈驱动下的 WSN 的病毒传播特点：当合法节点检出病毒的收益 a 大于其被病毒感染的损失 b 时，病毒传播的范围会不断扩张，直至所有节点都被感染，反之，病毒传播的范围会不断缩小，直至病毒消失。解释如下：由第 2 章的博弈模型可知，在攻防博弈中，恶意节点会以概率 *x**传播病毒，而合法节点会以概率 *y**进行检测，因此，感染概率为 $x^*(1-y^*)=\frac{ae_s}{(a+b)^2}$，治愈概率为 $x^*y^*=\frac{be_s}{(a+b)^2}$，当 *a*>*b* 时，感染速度大于治愈速度，病毒会在网络中蔓延，反之，当 *a*<*b* 时，感染速度小于治愈速度，网络感染节点的比例就会不断减小。值得指出的是，在判断某个博弈参数的变化对传播速度的影响时，不能只根据某一方可能采取的行动进行推断，而必须综合考虑双方的行动。例如，在 *a*>*b* 的情况下，当检测能耗 *es* 增大时，合法节点为了节约能量理应降低检测的概率，但这会促使恶意节点提高攻击概率，从而造成合法节点更大的损失，由混合纳什均衡策略可知，双方最终的博弈结果是合法节点保持检测概率不变，而恶意节点提高了攻击概率，从而使病毒的传播速度变快。

5　结束语

本文从博弈论的角度对 WSN 中的病毒传播过程进行了研究，得到了以下结论：a）WSN 中恶意节点与合法节点之间的攻防博弈模型存在混合纳什均衡解;b）WSN 中病毒传播结果与攻防博弈的收益参数有关，当合法节点检出病毒的收益大于其被病毒感染的损失时，感染比例会持续增加，直至所有节点都被感染，反之，感染比例会持续减少，直至所有恶意节点消失，该结论对制定抑制 WSN 病毒传播的措施具有一定的理论指导作用。

参考文献：

[1] 钱志鸿，王义君．面向物联网的无线传感器网络综述 [J]．电子与信息学报, 2013, 35(1): 215-227. (Qian Zhihong, Wang Yijun. Internet of Things-oriented Wireless Sensor Networks Review [J]. Journal of Electronics & Information Technology, 2013, 35(1): 215-227.)

[2] 洪锋，褚红伟，金宗科，等．无线传感器网络应用系统最新进展综述 [J]．计算机研究与发展，2010,47(S2): 81-87. (Hong Feng, Chu Hongwei, Jin Zongke, *et al.* Review of Recent Progress on Wireless Sensor Network Applications [J]. Journal of Computer Research and Development, 2010, 47(S2): 81-87.)

[3] 张焕国,韩文报,来学嘉,等．网络空间安全综述 [J]．中国科学:信息科学,2016, 46(2): 125-164. (Zhang Huanguo, Han Wenbao, Lai Xuejia, *et al.* Review of Cyberspace Security [J]. Scientia Sinica: Informationis, 2016, 46(2): 125–164.)

[4] 李化邓，李雷，施化吉，等．无线传感器网络的生存性评估[J]．计算机应用研究, 2018, 35(8): 2450-2453. (Li Huadeng, Li Lei, Shi Huaji, *et al.* Survivability evaluation in wireless sensor network [J]. Application Research of Computers, , 2018, 35(8): 2450-2453.)

[5] 沈士根，刘建华，曹奇英．博弈论与无线传感器网络安全 [M]．北京：清华大学出版社，2016.(Shen Shigen, Liu Jianhua, Cao Qiying. Game theory and wireless sensor network security [M].Beijing: Tsinghua University Press, 2016.)

[6] Abdalzaher M, Seddik K, Elsabrouty M, *et al.* Game theory meets

wireless sensor networks security requirements and threats mitigation: A survey [J]. Sensors. 2016, 16(7): 1-27.

[7] 沈士根，周海平，黄龙军，等. 基于最优反应均衡的传感网恶意程序传播抑制方法 [J].传感技术学报. 2017, 30(10):1589-1595. (Shen Shigen, Zhou Haiping, Huang Longjun, *et al.* Quantal Response Equilibrium-Based Method for Preventing WSN Malware Infection [J]. Chinese Journal of Sensors and Actuators, 2017, 30(10): 1589-1595.)

[8] Singh A, Awasthi A, Singh K, *et al.* Modeling and analysis of worm propagation in wireless sensor networks [J]. Wireless Personal Communications, 2018, 98(3) ,2535-2551.

[9] 张可径，曹奇英，沈士根. 基于演化博弈的 WSN 攻防策略选择动力学分析[J].计算机应用与软件, 2017, 34(9): 132-137. (Zhang Kejing, Cao Qiying, Shen Shigen. Dynamic analysis of attack and defense strategy selection for WSN based on evolutionary game[J].Computer Applications and Software, 2017, 34(9): 132-137.)

[10] 刘怡，林德钰. 基于进化博弈论的工业无线传感网能耗攻防研究 [J]. 测控技术, 2018, 37(4): 58-63. (Liu Yi, Lin Deyu. Defense against energy exhausting attack based on the evolutionary game theory for the industrial wireless sensor network[J]. Measurement and Control Technology, 2018, 37(4): 58-63.)

[11] Sedjelmaci H, Senouci S, Ansari N. Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a bayesian game-theoretic methodology [J].IEEE Trans on Intelligent Transportation Systems, 2017,18(5):1143-1153.

[12] 郑榕俊，陈志德，马金花.无线传感器网络中 n 蠕虫传播模型 [J]. 计算机应用. 2015, 35(S2):62-64. (Zheng Rongjun, Chen Zhide, Ma Jinhua. N-worm propagation model in wireless sensor networks [J]. Journal of Computer Applications, 2015, 35(S2): 62-64.)

[13] Shen S, Li H, Han R, *et al.* Differential game-based strategies for preventing malware propagation in wireless sensor networks [J]. IEEE Trans on Information Forensics and Security, 2014, 9 (11): 1962-1973.

[14] 周海平，蔡绍洪，龙艳. 个体差异对病毒传播效率的影响 [J]. 计算机应用研究, 2011, 28(10): 3797-3798. (Zhou Haiping Cai Shaohong, Long Yan. Effect of individual difference on virus'spreading efficiency [J]. Application Research of computers, 2011, 28(10): 3797-3798.)

[15] Wang T, Wu Q, Wen S, *et al.* Propagation Modeling and Defending of a Mobile Sensor Worm in Wireless Sensor and Actuator Networks [J]. Sensors, 2017,17(12):139-155.